Abstract Infrastructures of Unit Rank Two (Poster for ANTS VIII)

Felix Fontein
University of Zürich

June 12, 2008

Abstract

On our poster, we want to give information on the infrastructure of a global field of unit rank two. The infrastructure of a global field is the set of all minima of a fractional ideal, together with the neighbor relation and the baby step operations [HMPLR87, Fon08c]. In the case of unit rank one, it is both used for computation of fundamental units [Buc85a] and for cryptography [SSW96, JSS07].

One main emphasis lies on visualization, both of the set of minima together with baby steps (in the sense of J. Buchmann in [Buc85a]) and the generalized Voronoĭ algorithm. The generalized Voronoĭ algorithm was first described by J. Buchmann in [Buc85a, Buc85b] for number fields. In the case of purely cubic function fields, it has been introduced by Y. Lee, R. Scheidler and C. Yarrish in [LSY03]. Some screenshots of the current experimental version of our program can be seen on the second page; the shown cases are purely cubic function fields over $\mathbb{F}_5$. We also plan to present a live version on our laptop during the poster session.

Depending on our progress, we also plan to include new results on the unit rank two case [Fon08a], which are related to the interpretation of certain unit rank one infrastructures as cyclic groups as in [Fon08b].

References

[Buc85a] Johannes Buchmann. A generalization of Voronoĭ's unit algorithm. I. *J. Number Theory*, 20(2):177–191, 1985.

[Buc85b] Johannes Buchmann. A generalization of Voronoĭ's unit algorithm. II. *J. Number Theory*, 20(2):192–209, 1985.

[Fon08a] Felix Fontein. The infrastructure of a global field of arbitrary unit rank. In preparation.

[Fon08b] Felix Fontein. Groups from cyclic infrastructures and Pohlig-Hellman in certain infrastructures, 2008. To appear in Advances in Mathematics of Communications.

[Fon08c] Felix Fontein. The infrastructure of a global field of unit rank one, 2008. In preparation.

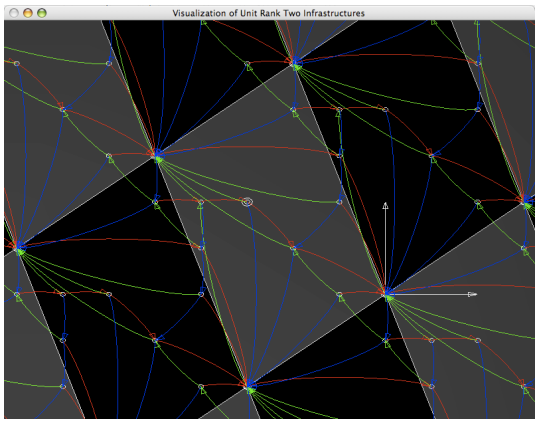
[HMPLR87] Y. Hellegouarch, D. L. McQuillan, and R. Paysant-Le Roux. Unités de certains sous-anneaux des corps de fonctions algébriques. *Acta Arith.*, 48(1):9–47, 1987.

[JSS07] M. J. Jacobson, R. Scheidler, and A. Stein. Cryptographic protocols on real hyperelliptic curves. *Adv. Math. Commun.*, 1(2):197–221, 2007.

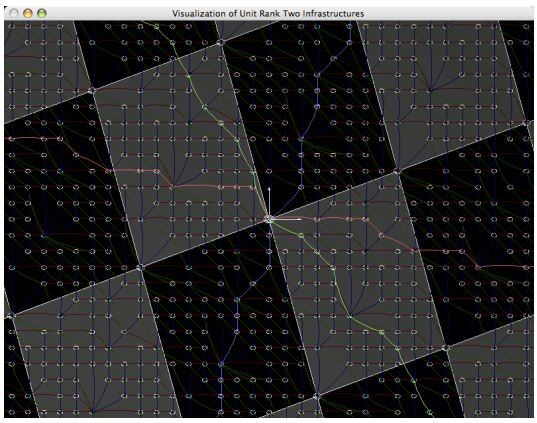
[LSY03] Y. Lee, R. Scheidler, and C. Yarrish. Computation of the fundamental units and the regulator of a cyclic cubic function field. *Experiment. Math.*, 12(2):211–225, 2003.

[SSW96] R. Scheidler, A. Stein, and Hugh C. Williams. Key-exchange in real quadratic congruence function fields. *Des. Codes Cryptogr.*, 7(1-2):153–174, 1996. Special issue dedicated to Gustavus J. Simmons.

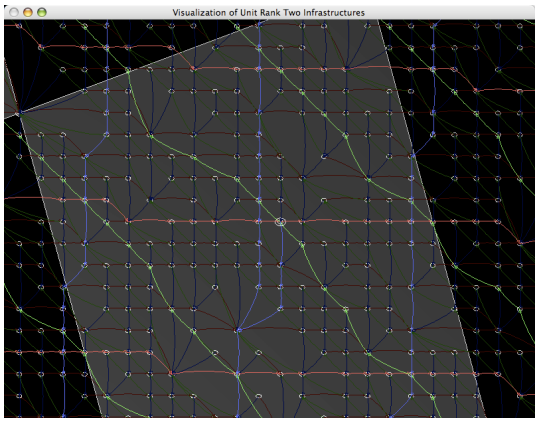
Preview from Current Visualization Experiments



All minima with baby steps in all three different directions drawn.



The (two sided) Voronoĭ chains of 1 in different directions.



The Voronoĭ chains of a minimum together with their translates by the action of the unit group. In the blue direction, it has a non-trivial pre-period.

In all pictures, every second translate of a fundamental parallelotope of the unit lattice is drawn in gray.

Each point's x-coordinate is the first valuation at infinity, and the y-coordinate is the second valuation at infinity. Red baby steps go in the direction of the first valuation, green baby steps into the direction of the second, and blue baby steps in the direction of the third.